Wind River Payments

SecureTrust SAQ A Instruction Guide

Purpose: These instructions will assist in registering your account for PCI compliance, validating PCI Compliance readiness, and completing the annual PCI questionnaire.

Payments. Your Way.

Contents

SAQ A Instructions

1. Click **Begin Step.**

2. Click **Start Business Profile.**

3. Click the circle next to "**Expert**" and then click **Next**.

Pick an assessment method

○ Guide Me - Choose this option to receive step-by-step guidance throughout the compliance validation process. Next series of questions will help determine your PCI scope. Your PCI scope is used to ensure the right PCI requirements for your business type are covered.

→ ○ Expert - Choose this option to be able to select from a list of available PCI SAQ forms to complete without step-by-step guidance. Next series of questions will help recommend a SAQ form.

○ Upload - Choose this option if you are already certified with another provider and need to upload your compliance documents to this account

NEXT

4. Click the circle next to "**Self Assessment Questionnaire (SAQ) A**" and click **Next**.

Your current valid PCI DSS compliance assessment type

Please select the PCI DSS compliance assessment type that you are submitting from the selection below.

→ ◉ Self Assessment Questionnaire (SAQ) A

○ Self Assessment Questionnaire (SAQ) A-EP

○ Self Assessment Questionnaire (SAQ) B

○ Self Assessment Questionnaire (SAQ) B-IP

○ Self Assessment Questionnaire (SAQ) P2PE

○ Self Assessment Questionnaire (SAQ) C-VT

○ Self Assessment Questionnaire (SAQ) C

○ Self Assessment Questionnaire (SAQ) D

○ Self Assessment Questionnaire (SAQ) D-Service Provider (upload only)

○ Report on Compliance (upload only)

PREVIOUS   **NEXT**

5. If scanning is required in your environment, select **Yes.**

Does your compliance assessment require scanning?

Is quarterly scanning a requirement of your PCI DSS compliance assessment, otherwise referred to as an ASV External Vulnerability Scan?

○ Yes   ○ No

PREVIOUS   NEXT

6. Answer the **Third-Party Payment Service Providers** question.

Third-party payment service providers

Do you have relationships with one or more third-party service providers that store, process, or transmit account data on your company's behalf (for example, payment gateways, payment processors, payment service providers (PSPs), and off-site storage)?   ❓

○ Yes   ○ No

PREVIOUS   NEXT

7. Answer the **Password Policy** question.

Password policy

Do you enforce a minimum password length of seven characters, containing both numeric and alphabetic characters, for user accounts on all POS devices, computers and systems in your business?   ❓

○ Yes   ○ No

Please note: After 31st March 2025, you will need to enforce a minimum password length of twelve characters (where twelve characters are supported, otherwise a minimum of eight characters is required). This also applies to passwords used by all non-customer users and administrators with access to e-commerce websites/webservers.

PREVIOUS   NEXT

8. Fill out the summary information then click **Next**.

A summary of how and where you handle card payments

Please provide the information requested below. This will form part of your Attestation of Compliance

List your business premises type(s) and a summary of locations that are relevant to your PCI DSS assessment (eg, retail outlets, corporate offices, data centres, call centres etc..)

0/4000

Generally, how does your business store, process and/or transmit cardholder data?

0/4000

Briefly describe the environment and/or systems covered by this assessment

0/4000

PREVIOUS   NEXT

9. Click **Manage** in the **Complete Security Assessment** box.

Here are your available compliance tools

Your business profile
Complete
SAQ type A

MORE INFO   MANAGE

Be scan compliant
PCI DSS External Vulnerability Scan result has expired

MORE INFO   MANAGE

Complete security assessment
25 Unanswered questions
0 Remediation tasks

MORE INFO   MANAGE

5

10. Click **Answer Now.**

11. Answer all the unanswered questions (the number of questions may vary).
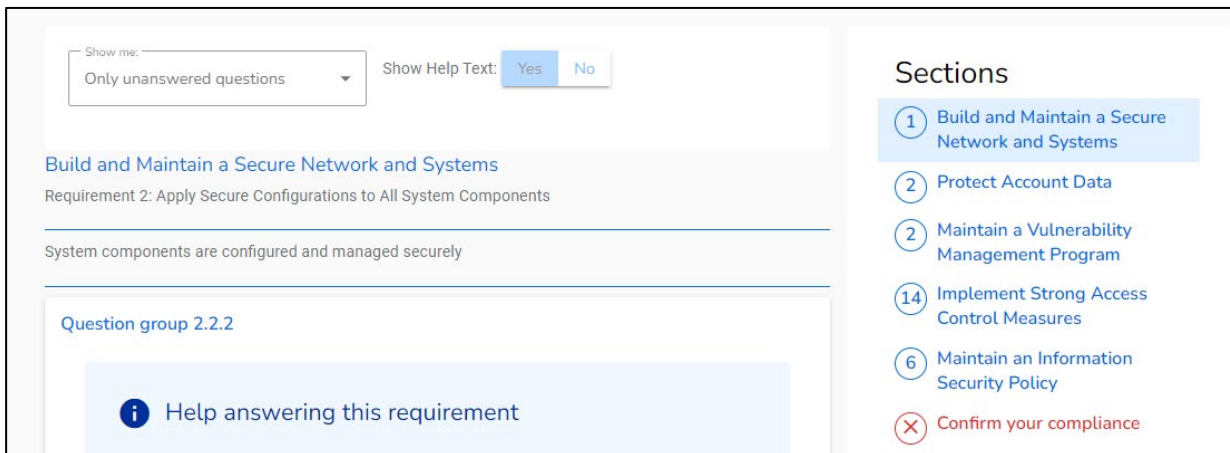
12. Click **Confirm Your Compliance** (if not already in that section).

13. Click **Confirm Your Attestation**.

SAQ A Renewal Instructions

1. Click **Manage** in the **Complete Security Assessment** box.
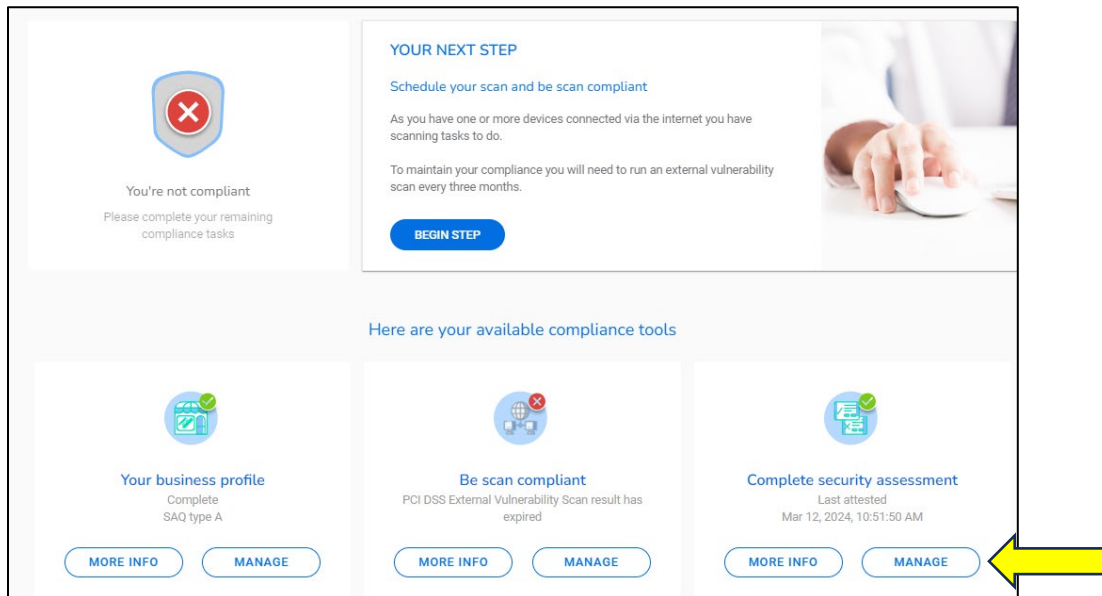
2. Click **Answer Now.**
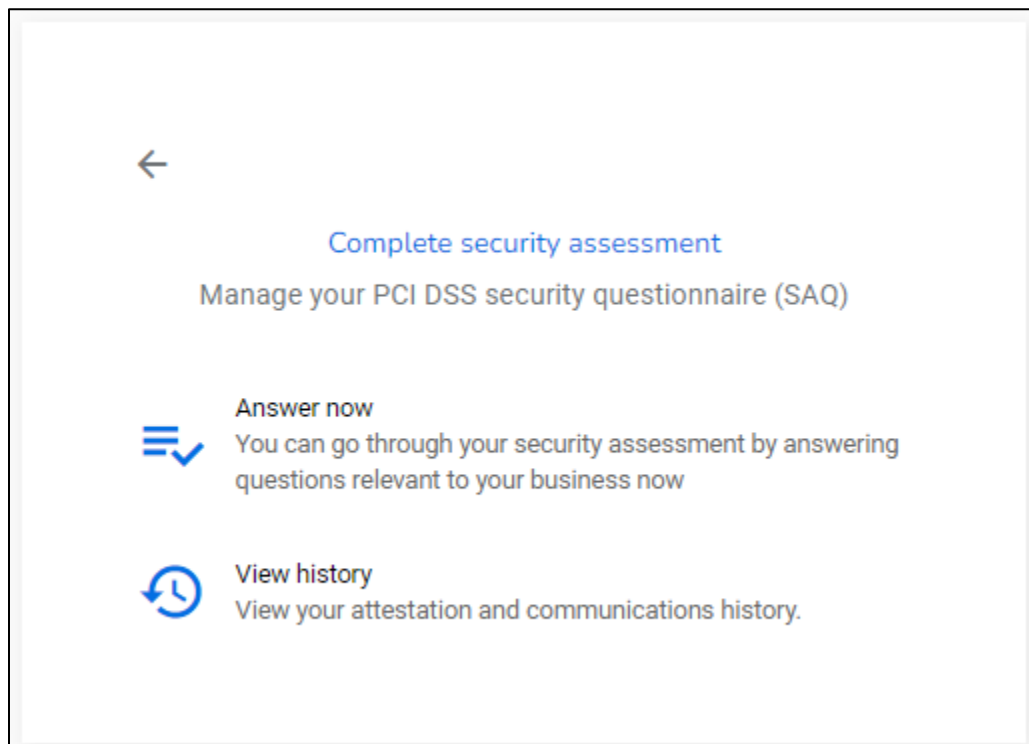
3. Click the **Confirm Your Compliance** in the Sections box.

4. Scroll down to the Attestation Box and click **Confirm Your Attestation** (it may also say nothing has changed).

Schedule a Scan Instructions
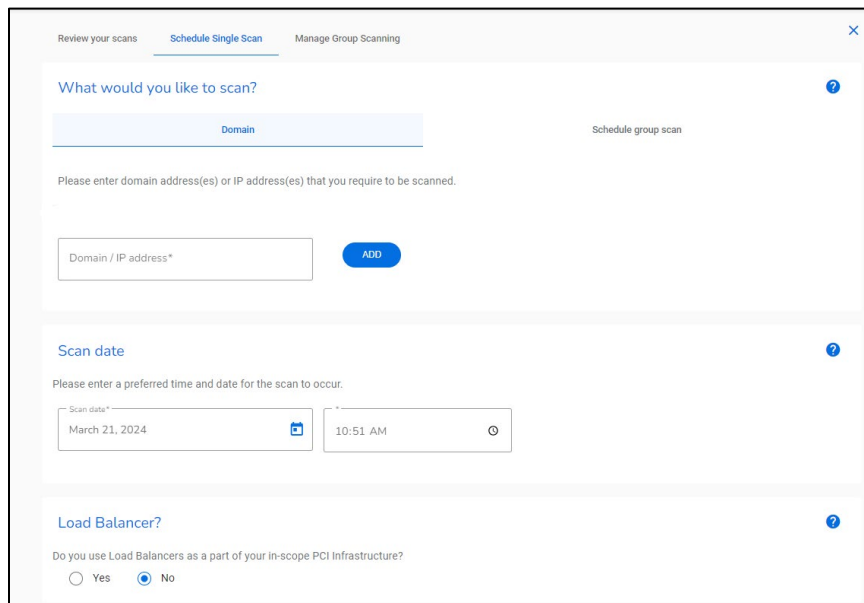
1. If your environment requires scans, the portal will prompt for scans after completing the business profile. Click **Manage** in the **Be Scan Compliant** box to get started.
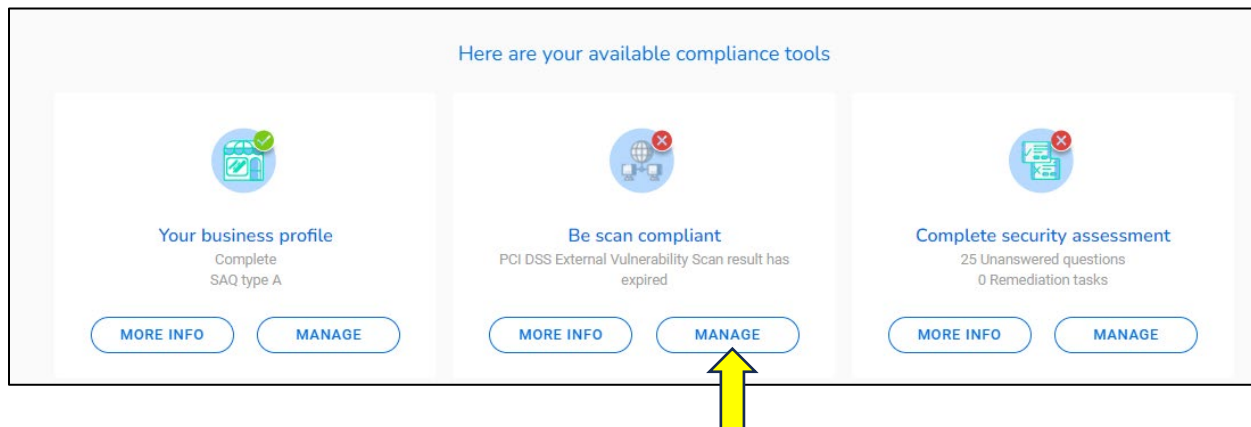
2. Click **Schedule a Scan.**
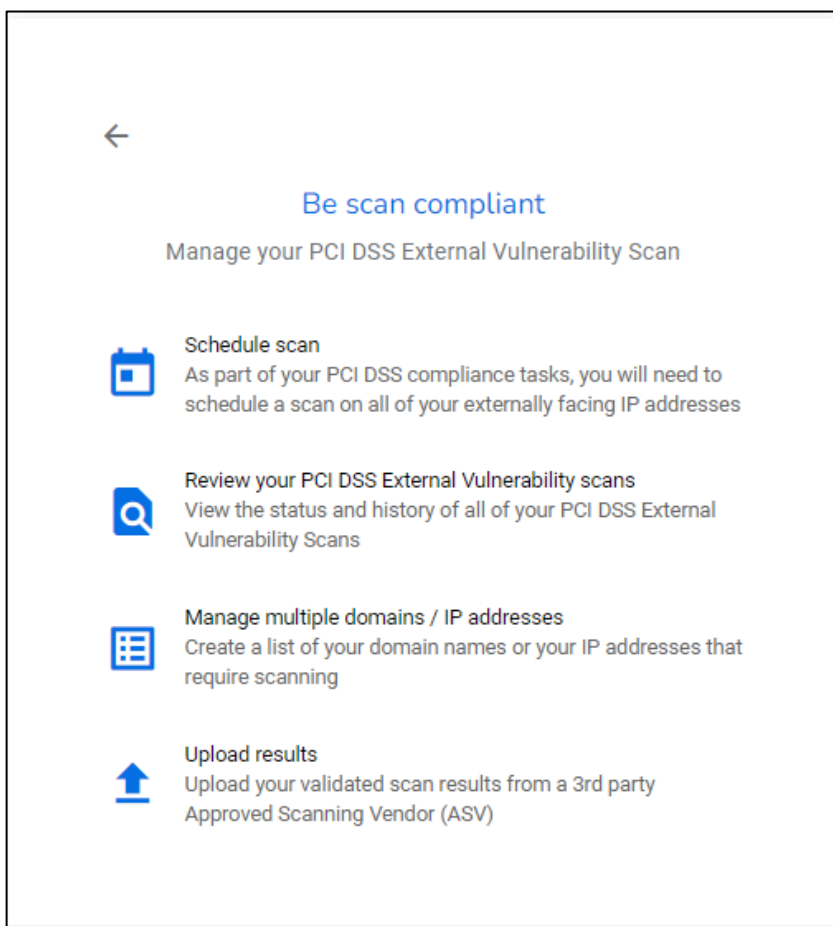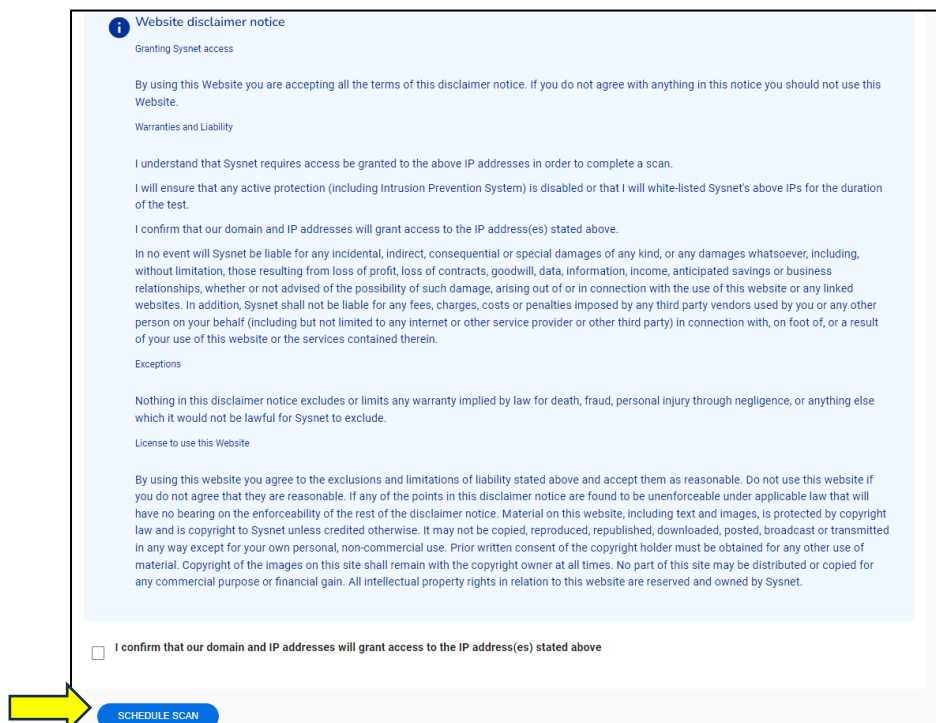
3. Fill in the IP Address(es) that need to be scanned.

2. Click the box confirming your domain and click **Schedule Scan**.

3. After the scan is completed, the results will be emailed to your contact information on file. Review those to confirm the scan was successful or take any required steps to finalize the scanning process.